

Honorable J Richard Creatura

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON

NATHEN BARTON,

Plaintiff  
v.

JOE DELFGAUW, XANADU  
MARKETING INC., EXPERIAN  
INFORMATION SOLUTIONS INC.,  
STARTER HOME INVESTING INC, &  
JOHN DOE 1-10  
Defendant(s).

CASE NO. **3:21-cv-05610-JRC**

MOTION FOR SUMMARY  
JUDGEMENT ON DEFENDANTS  
COUNTERCLAIM

NOTE ON MOTION CALENDAR:  
July 8, 2022

ORAL ARGUMENT REQUESTED

PLEASE TAKE NOTICE that Plaintiff Nathen Barton (hereinafter referred to as “Plaintiff”) moves the Court to for summary judgement on Defendants’ counterclaims.

**I. INTRODUCTION**

At the heart of this case is consent – Did the Defendants telemarket Barton without consent or invitation, *or* did Barton fraudulently “opt in” with the hope that the Defendants would telemarket Barton and Barton could sue them.

1 The Defendants have a story – someone “opted in” with a name and telephone number on  
 2 their website [educationschoolmatching.com](http://educationschoolmatching.com)<sup>1</sup>, and they solicited that number. They claim the IP  
 3 address of the person who “opted in” is 71.238.123.34, and they found a website (*iplocation.net*)  
 4 that says that IP address points back to a [GPS coordinate](#) a few miles from Plaintiff’s house.

5 Their story has issues – The “opt-in” IP address claim of 71.238.123.34 is hearsay and  
 6 without foundation. No witnesses the Defendants identified in the case have personal knowledge  
 7 of the IP address of who (if anyone<sup>2</sup>) “opted in”. Someone (who Defendants could not name in a  
 8 deposition) told them that 71.238.123.34 was the “opt in” IP address.

9 The report they found on *iplocation.net* has the same problem – it is hearsay and the  
 10 Defendants choose to forgo having a witness lay a foundation for the admissibility of the report.

11 The *iplocation.net* reports were generated at least six months after the alleged “opt in”.

12 Last, the report points to a variety of locations up to thousands of miles away, and at the  
 13 bottom of the report it has a large disclaimer warning the reader that locations shown may be  
 14 accurate only to the *country* level.

15 No reasonable juror could find that Plaintiff consented (“opted in”) to receive telephone  
 16 solicitation which negates an essential element of all counterclaims.

### 17 **Authenticated Document and Hearsay Standard in Summary Judgement**

---

18  
 19  
 20 <sup>1</sup> Attached as Exhibit A.

21 <sup>2</sup> Plaintiff does not know if anyone “opted in”. Plaintiff asked Defendants who could vouch for  
 22 the accuracy of their “opt in” information and they answered Joseph Delfgauw and Edward  
 23 Winkler. During their depositions, both testified that they had no personal knowledge of the  
 24 accuracy of their “opt in” information. See Dkt. 167. Plaintiff believes it is quite possible  
 Defendants found an IP address as close to Plaintiff’s location as possible and said that was the  
 “opt in” IP address. It would explain why no employee of the Defendants was willing to be  
 named as a witness and risk being deposed.

"We have repeatedly held that unauthenticated documents cannot be considered in a motion for summary judgment. See *Cristobal v. Siegel*, 26 F.3d 1488, 1494 (9th Cir. 1994); *Hal Roach Studios, Inc. v. Richard Feiner Co., Inc.*, 896 F.2d 1542, 1550-51 (9th Cir. 1989); *Beyene*, 854 F.2d at 1182; *Canada v. Blain's Helicopters, Inc.*, 831 F.2d 920, 925 (9th Cir. 1987); *Hamilton v. Keystone Tankship Corp.*, 539 F.2d 684, 686 (9th Cir. 1976)." *Orr v. Bank of America*, NT & SA, 285 F.3d 764, 773 (9th Cir. 2002)

'Hearsay is "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." Fed.R.Evid. 801(c). In the absence of a procedural rule or statute, hearsay is inadmissible unless it is defined as non-hearsay under Federal Rule of Evidence 801(d) or falls within a hearsay exception under Rules 803, 804 or 807. See Fed.R.Evid. 802; 30B Federal Practice Procedure: Evidence § 7031 at 279.' *Orr v. Bank of America*. Emphasis added.

## II. WHY SUMMARY JUDGEMENT OF THEIR CLAIMS IS APPROPRIATE

- a) Defendants base their allegation that Plaintiff "opted in" from IP address 71.238.123.34 solely on a document called *Table B* in Dkt. 167. However, as Dkt. 167 outlines, Defendants cannot authenticate *Table B* according to Fed. Rule. Evidence 901(b)(1) and *Table B* is hearsay that cannot be authenticated under another rule. *Table B* being inadmissible, Defendants do not know the IP address of who (or what) "opted in".
- b) Based on geolocating IP address 71.238.123.34, defendants allege Plaintiff "opted in" from a specific physical location (or locations) at specific dates and times. This allegation fails because:

1. The Defendants use an IP Geolocation report from *iplocation.net* to attempt to prove IP address 71.238.123.34 was assigned to a subscriber a few miles from Plaintiff's

1 residence. They then would ask the Court to make the leap that if the subscriber  
2 who “opted in” lived a few miles from Plaintiff’s residence, Plaintiff must be the  
3 source of the “opt in”. This report suffers from the same admissibility problem as  
4 *Table B* – Defendants cannot authenticate the document, and it is hearsay, so it is  
5 not admissible.

6 2. Further, even if 1) were not an issue, IP Geolocation is very inaccurate, the  
7 Defendants own document disclaims the accuracy of the locations shown, the IP  
8 Geolocation document they rely on is dated at least six months after they allege the  
9 “opt ins” took place, and the only complete version of that document they have  
10 shows the IP address might belong to a subscriber in New Jersey.

11 3. Finally, Defendants have no evidence Plaintiff was at *any* particular location at the  
12 dates and times they allege. Plaintiff testifies he was not at or nearby any location  
13 identified by Defendant on the day any of the alleged “opt ins” occurred. Plaintiff  
14 further testifies he never “opted in” to solicitation calls from Defendants at any time,  
15 in any place, using any method, never asked anyone else to do so on his behalf, and  
16 is unaware of anyone who would do so, or did do so. Defendants have no evidence  
17 to the contrary.

18 c) Plaintiff testifies that he has never used (or asked anyone else to use, and is not aware of  
19 anyone else using) IP address 71.238.123.34 at any time relevant to this lawsuit.  
20 Defendants have no evidence to the contrary.

d) Defendants allege Plaintiff “opted in” with email address

[ivettealfredomartinez@gmail.com](mailto:ivettealfredomartinez@gmail.com). This email address is not random – it belongs to a previous subscriber of the phone number and does not appear to be public information. Plaintiff has testified he had never seen this email address before Defendants showed it to him in discovery. Defendants have no evidence to the contrary.

e) Joe Delfgauw, party to this lawsuit, has a more logical explanation – a “form spammer” opted in with real information.

### III. DEFENDANTS IP INFORMATION IS HEARSAY AND CANNOT BE AUTHENTICATED

This section is a summary of the motion in Dkt.167 that covers this issue in greater detail. Essentially, Plaintiff asked Defendants for all facts and evidence Plaintiff “opted in” and they responded with two documents, Table A being the first.

*Table A*

ID	Campaign	Day/Time	First	Last	Phone	Email	Actions
367588486	12130	2021-04-30 15:50:09	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com	<a href="#">View</a>
367588483	12130	2021-04-30 15:50:08	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com	<a href="#">View</a>
362407192	12130	2021-04-13 17:58:07	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com	<a href="#">View</a>
362407183	12130	2021-04-13 17:58:02	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com	<a href="#">View</a>
361284364	13690	2021-04-09 18:29:38	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com	<a href="#">View</a>
358819495	3824	2021-04-01 14:04:11	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com	<a href="#">View</a>

A second related document (Table B) contained the information of Table A with the addition of the IP address of each alleged “opt in”.

*Table B*

id	campaign_id	first	last	phone	email	ip	datetime
358819495	3824	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com	71.238.123.34	4/1/2021 14:04
361284364	13690	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com	71.238.123.34	4/9/2021 18:29
362407183	12130	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com	8.8.8.8	4/13/2021 17:58
362407192	12130	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com		4/13/2021 17:58
367588483	12130	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com	8.8.8.8	4/30/2021 15:50
367588486	12130	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com		4/30/2021 15:50

Table B is the only evidence in the entire controversy with IP address information.<sup>3</sup>

In Depositions held on May 18, 2022, Edward Winkler (“Winkler”) and Joe Delfgauw (“Delfgauw”) each testified<sup>4</sup> that they themselves cannot personally attest to the accuracy of the information in *Table B*, and said other persons (that they could not name during the deposition) were the source of the document but they were not certain as to who.

### Sidebar

On 6/13/2022, 10 days after the deadline for all discovery related motions, and 9 days before the discovery completion date, Defendants filed an updated witness list (Dkts. 170 & 171). This seems prompted by Dkt. 167. However, on March 24, 2022, Defendants had just answered that only Winkler and Delfgauw could testify to the veracity of Table A (the document referred to below). Plaintiff reminds the Court that the only difference between Table A and Table B is that Table B adds IP addresses.

#### INTERROGATORY NO. 16:

You turned over the following document. Give the name and address of every person who can swear under penalty of perjury that no piece of data in this document has been doctored.

#### RESPONSE TO INTERROGATORY 16:

Edward Winkler – Mail can be sent to 956 3 Mile Road N.W., Grand Rapids  
MI 49544

Joe Delfgauw – Mail can be sent to 956 3 Mile Road N.W., Grand Rapids  
MI 49544

Previous to filing Dkts. 170 & 171, Opposing Counsel knew that Plaintiff had a pre-paid, long planned trip that would take six of those nine days. See the associated Declaration of Nathen Barton, ¶10-¶11.

<sup>3</sup> Table B shows “opt ins” from IP address 8.8.8.8, Google’s public DNS server. See Dkt. 121. Delfgauw testified that Table B is inaccurate – no “opt in” was from 8.8.8.8. See Dkt. 168, 4:17 to 5:10. This alone shows Table B is fundamentally inadmissible due to the “best evidence” rule.

<sup>4</sup> Winkler Deposition – see Exhibit H – Starting at Page 5, Line 10 through Page 6, Line 15.

Delfgauw Deposition – See Exhibit C – Starting at Page 49, Line 16 (the discussion is about Table B), through Page 60, Line 13..

Defendants were the sole custodian of who on their side had discoverable information. This Court has the power to exclude any and all witnesses they chose not to disclose unless the omission was substantially justified or harmless.

“[W]e give particularly wide latitude to the district court's discretion to issue sanctions under Rule 37(c)(1),” which is “a recognized broadening of the sanctioning power.” *Yeti by Molly, Ltd. v. Deckers Outdoor Corp.*, 259 F.3d 1101, 1106 (9th Cir.2001) ; see also *R & R Sails*, 673 F.3d at 1245 (same); *Jeff D. v. Otter*, 643 F.3d 278, 289 (9th Cir.2011) (“[A] district court has wide discretion in controlling discovery.”) (alteration in original) (internal quotation marks omitted). *Ollier v. Sweetwater Union High Sch. Dist.*<sup>5</sup>, 768 F.3d 843, 859 (9th Cir. 2014).

*Ollier* is almost directly on point with this case.

“Orderly procedure requires timely disclosure so that trial efforts are enhanced and efficient, and the trial process is improved. The late disclosure of witnesses throws a wrench into the machinery of trial. A party might be able to scramble to make up for the delay, but last-minute discovery may disrupt other plans. And if the discovery cutoff has passed, the party cannot conduct discovery without a court order permitting extension. This in turn threatens whether a scheduled trial date is viable. And it impairs the ability of every trial court to manage its docket.” *Ollier*.

### **End of Side Bar**

This leaves *Table B* (and *Table A*) without a witness who can lay a foundation for the admissibility of the document. Defendants named only three witnesses in their timely FRCP 26 disclosure – Winker, Delfgauw, and Alex Jakimtschuk (“Jakimtschuk”). Jakimtschuk works for a different Delfgauw company and has no ability to lay a foundation for *Table B* or *Table A*<sup>6</sup>.

<sup>5</sup> <https://casetext.com/case/ollier-v-sweetwater-union-high-sch-dist-4>

<sup>6</sup> Plaintiff points out that Jakimtschuk was removed completely from Dkts. 170 & 171 – their updated witness lists.



Without someone who can lay a foundation for *Table A* or *Table B*, these documents are inadmissible, and Defendants have no evidence of any IP address at all.

Defendants also do not know how to handle IP address 8.8.8.8. Delfgauw testified there was no “opt in” was from 8.8.8.8. See Exhibit C (Delfgauw’s Deposition) Page 39, Lines 15-19. The discussion is about *Table B*. Skip ahead to Page 40, Lines 2-12. Skip ahead to Page 40, Line 20 – Page 42, Line 3. On the other hand, they gave this admission<sup>7</sup>. Plaintiff made their conflicting answers it easy to see the attached Exhibit J. Exhibit J shows the Defendants can’t agree if there were opt-ins from 8.8.8.8, or not. Plaintiff has testified in the attached Declaration that he does not use 8.8.8.8. ¶14-¶16.

14	<b><u>ADMISSION NO. 107:</u></b>	Admit or deny that the entity who “opted in” from IP address
15		71.238.123.34 is the same entity who opted in from IP address 8.8.8.8.
16	<b><u>ANSWER:</u></b>	
17		Counterclaimant admits that Plaintiff/Counter defendant opting-in from IP Address
18		71.238.123.34 and provided the same information when opting-in 29 days later the
19		Google proxy connection 8.8.8.8 According to <a href="https://www.ipqualityscore.com">https://www.ipqualityscore.com</a> , IP
		address (8.8.8.8) is a proxy connection and is associated with recent SPAM blacklist
		activity or abusive behavior.

This inability of Defendants to decide if someone “opted in” from 8.8.8.8 or if Defendants corrupted their own “opt in” records shows *Table B* is fundamentally inadmissible.

#### IV. DEFENDANTS HAVE NO IP GEOLOCATION ADMISSIBLE EVIDENCE

Defendants have only offered evidence from IP Geolocation website *iplocation.net* to attempt to connect Plaintiff to IP address 71.238.123.34. The Defendants chose not to identify a witness<sup>8</sup> who can lay a foundation for the admissibility of any IP Geolocation report, all IP

<sup>7</sup> 12.7.2021 CD Delfgauw Admissions 8

<sup>8</sup> Defendants chose not to use an expert witness.

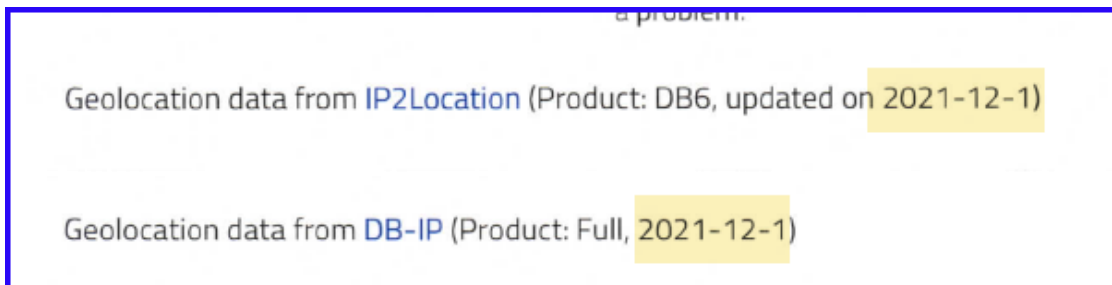


Geolocation documents are hearsay, and the *iplocation.net* report specifically can't fit into a hearsay exception of Fed. R. Evidence [801\(d\)](#), Rules [803](#), [804](#) or [807](#).

***iplocation.net* Report is inadmissible**

It appears that Defendants first printed the *iplocation.net* report sometime in October 2021. Dkt. 154 addressed how the Defendants took this October<sup>9</sup> *iplocation.net* report, cut it down to one page, and presented it as evidence in this case. That one-page document indicates it was sourced during or after October 2021.

Inside the *iplocation.net* reports there are date codes. For example, Exhibit B (Dkt. 104-2) contains the data from a product updated on December 1, 2021 and another product dated December 1, 2021. Clearly Dkt. 104-2 was obtained on or after December 1, 2021.



Defendants never did turn over the original, full, and unmodified October dated report to Plaintiff or the Court. The earliest complete<sup>10</sup> *iplocation.net* report Defendants turned over to Plaintiff and the Court is Dkt. 104-2. It is attached to this Motion as Exhibit B.

Defendants could only argue that these *iplocation.net* reports are admissible under [803\(17\)](#) Market Reports and Similar Commercial Publications.

<sup>9</sup> It is unknown how often this report changes. Perhaps every day. Plaintiff refers to the “month” of the *iplocation.net* report not because he affirms that the report only changes month to month, but because inside the report itself, a date appears to change each calendar month.

<sup>10</sup> Any incomplete or modified *iplocation.net* report would be inadmissible under the “[best evidence](#)” rule.

1 However, the Court would have to find these *iplocation.net* reports reliable and  
 2 necessary, and the Defendants would have to show the information in them is authentic. None of  
 3 these hurdles can be overcome. From the Defendants' own Dkt. 104-2 (bottom of page 5)<sup>11</sup>:

4 "The Geolocation lookup tool provided on this page is an estimate of where the IP  
 5 address may be located."

6 "The data come from a few IP-Based Geolocation providers, and their accuracy varies  
 7 depending on how quickly they update their database when changes occur. Since many  
 8 Internet users are getting their dynamic IP address<sup>12</sup> from their ISP, and most ISPs serve  
 9 their customers in multiple regions causing Geolocation lookup to be accurate to the  
 10 region they serve."

11 "For example, AT&T in the United States serve their customers in entire USA and the  
 12 accuracy may be limited to the Country level."

13 Other ISPs may be serving smaller areas, and some ISPs create subnetworks to serve  
 14 their customers in smaller regions. For this reason, the IP-based Geolocation will be  
 15 about 99% accurate at the country level while the accuracy of State and City may be at  
 16 much less accurate level somewhere around 50% range." Emphasis added.

17 Reliability and necessity are requisite for this document to fall under the [803](#)(17) hearsay  
 18 exception<sup>13</sup>. The disclaimer in Dkt. 104-2 screams unreliability:

- 19 • This report admits it pulls the information from "a few IP-Based Geolocation  
 20 providers". Exhibit B is hearsay sourced from hearsay. Where do those providers  
 21 get their information?

22 <sup>11</sup> Dkt. 104-2 has an obstruction over some of this text. Defendants turned over later versions of this  
 23 document will all of this text visible.

24 <sup>12</sup> It is undisputed that 71.238.123.34 is a Comcast dynamic IP address (Dkt. 55).

<sup>13</sup> Weinstein's Federal Evidence says:

As with other hearsay exceptions, the admissibility of market reports and commercial  
 publications under Rule 803(17) is predicated on the two factors of necessity and reliability.  
 Necessity lies in the fact that if this evidence is to be obtained it must come from the  
 compilation, since the task of finding every person who had a hand in making the report or list  
 would be impossible. Reliability is assured because the compilers know that their work will be  
 consulted; if it is inaccurate, the public or the trade will cease consulting their product.

- “their accuracy varies depending on how quickly they update their database when changes occur” (update frequency is unknown)
- most ISPs serve their customers in multiple regions causing Geolocation lookup to be accurate to the region they serve. (Comcast serves 40 states)
- “the accuracy of State and City may be at much less accurate level somewhere around 50% range (lack of foundation means this number is speculation)

Who could rely on such a long list of caveats and accuracy warnings? The accuracy notice about ISPs operating in multiple regions is particularly on point here – Comcast serves a large region of the USA – 40 states<sup>14</sup> – and in 2021 had 34.2 million subscribers<sup>15</sup>.

Dkt. 104-2 warns the reader the locations shown for 71.238.123.34 (a Comcast IP address) are only accurate to somewhere within the 40 states Comcast operates. Plaintiff notes for the Court that 104-2 pointed to a New Jersey location and Comcast operates in there.

### ***iplocation.net* Report is Out of Date**

Noted two pages previously, Dkt. 104-2 was obtained on or after December 1, 2021.

On 11/22/2021, Plaintiff in Dkt. 49 moved the Court to order Comcast Inc. to disclose the subscriber information for IP address 71.238.123.34. Defendants opposed Dkt. 49 and on January 5, 2022, the Court denied the motion with the explanation (Dkt. 96, 3:8-15):

“Dynamic IP addresses<sup>16</sup> are IP addresses that may be reassigned periodically to different subscribers. See *Call of the Wild Movie, LLC v. Does 1-1*, 062, 770 F. Supp. 2d 332, 356 (D. D.C. 2011) (“[F]or dynamic IP addresses, a single IP address may be re-assigned to many different computers in a short period of time.”).

Thus, the IP address identified by plaintiff might have been assigned to multiple individuals over the last six months and any response Comcast could provide would not

---

<sup>14</sup> See Exhibit D.

<sup>15</sup> Taken from Comcast’s 2021 10-K SEC filing (page 5) located at <https://www.cmcsa.com/static-files/8887f574-dfa9-4480-8c8b-ed7771f7ce44>

<sup>16</sup> It is undisputed that 71.238.123.34 is a Comcast dynamic IP address (Dkt. 55).

1 contain information of who used the IP address in or before April 2021, the period he is  
2 alleged to have opted in.”

3 This Court has already found that by late 2021, this IP address might have been assigned  
4 to multiple individuals in the preceding six months. Exhibit B is also inadmissible due to being  
5 irrelevant - way out of date.

#### 6 **V. PLAINTIFF TESTIFIES HE NEVER USED IP ADDRESS 71.238.123.34**

7 Plaintiff testifies in the associated Declaration that to his knowledge he has never used IP  
8 address 71.238.123.34. ¶6.

9 Plaintiff testifies in the associated Declaration that he did not “opt in” at any time on  
10 *educationschoolmatching.com*. ¶3.

11 Plaintiff testifies in the associated Declaration that he did not ask anyone else to “opt in”  
12 at any time on *educationschoolmatching.com*. ¶4.

13 Plaintiff testifies in the associated Declaration that does not know of anyone who has  
14 “opted in” at any time on *educationschoolmatching.com*. ¶5.

#### 15 **VI. PLAINTIFF TESTIFIES HE WAS NOT AT ANY “OPT IN” LOCATION ON 16 ANY DAY OF ANY ALLEGED “OPT IN”**

17 Plaintiff testifies in the associated Declaration that he was not at any location Defendants  
18 alleged was an “opt in” location on the day of any alleged “opt in”. Plaintiff testifies in the

#### 19 **Telemarketing Lingo - affiliate marketing**

20 Affiliate marketing is the process by which an affiliate earns a commission for marketing  
21 another person’s or company’s products. In this case, the product is “opt ins” on  
educationschoolmatching.com.

#### 22 **Telemarketing Lingo – Form Spammer**

23 A form spammer is an affiliate marketer gone rogue. In this case, the form spammer  
24 himself could fill out the “opt in” form on educationschoolmatching.com with names and  
phone numbers to earn a commission. This can be done via a computer program – a  
“bot”.

1 associated Declaration that he was not within miles of any location Defendants alleged was an  
2 “opt in” location on the day of any alleged “opt in”. ¶7.

3 **VII. IF ANYONE “OPTED IN”, IT WAS A FORM SPAMMER**

4 Defendant Delfgauw testified in his 5/18/2022 deposition that he is the [CEO](#)<sup>17</sup> of the  
5 business [Validiform.com](#). During this deposition, he testified that:

- 6 1. Delfgauw was aware that bots and people are out there “opting in” to get paid  
7 (form spammers).  
8 2. Delfgauw paid affiliate marketers to deliver “opt ins” to  
9 [educationschoolmatching.com](#)  
3. Delfgauw never looked to see if he paid an affiliate marketer for the “opts ins” in  
question.

10 Starting at Exhibit C, Page 23, Line 24:

11 Q. On Validiform.com it says that you're the CEO of Validiform. Is that a true statement?

12 A. I am. It is.

13 **Skipping ahead to page 24, line 19**

14 Q. Are you aware of the blog that is on Validiform?

15 A. I'm not aware at this very moment of a blog --what the blog says. I mean I am --  
16 hopefully there is a blog.

17 **Skipping ahead to page 26, line 25 (emphasis added)**

18 Q. So on Validiform, would it surprise you to learn that the blog talks in detail about the  
spam bot opting in with real stolen information?

19 A. So it is commonly known in the marketing world that there are companies out there that  
20 try to get paid to absolutely enter in false information, whether it's a bot, whether it's a  
21 person. That's a pretty commonly known thing, yes. I don't know if that was your  
22 question, by the way. Sorry.

23  
24 <sup>17</sup> Exhibit G, Page 4

1 Q. I think that's good enough for the minute. Do you pay anyone to deliver opt-ins to any  
2 of your web sites? Like are you paying people to deliver opt-ins?

3 A. Yes. We have an affiliate network called the Mountain Top Network that hosts and  
4 promotes all the web sites.

5 Q. So if I told you that the alleged opt-in -- or I'll say alleged, because honestly, I don't  
6 know if it's alleged or not. Would it surprise you to learn that the alleged opt-in in this  
7 lawsuit happened on educationmatching.com?

8 A. Educationschool?

9 Q. Oh. Educationschoolmatching.com. Would it surprise you to learn that that is the source  
10 of the alleged opt-in?

11 A. You want me to answer?

12 Q. Yes, please.

13 A. Would it surprise me? If I can say this without -- nothing surprises me.

14 Q. Okay.

15 A. I mean I hate to say that. I mean I have seen all kinds of weird stuff in this, so not much  
16 surprises me.

17 Q. Is that a web site that some of your affiliates can get paid by delivering opt-ins?

18 A. Yes. Educationschoolmatching.com is an opt -- an offer where someone can get paid to  
19 drive traffic to the web site that has a verified source.

20 Q. Do you know if the opt-in in question in this lawsuit resulted in someone getting paid  
21 for that opt-in?

22 A. I don't know off the top of my head.

23 Q. Okay. So just to be sure I ask a correct question, did you pay someone for the opt-in in  
24 question?

A. I can find out, but I don't know off the top of my head.

Q. And you never looked previously to see if you paid someone for this opt-in?

A. I have not looked, but it's possible -- let me back up. It's possible we looked. I don't  
remember if we looked.

1. At this point it has been established that Delfgauw pays affiliate marketers to deliver “opt ins” to the website Defendants allege the “opt ins” occurred.
2. Delfgauw expected Validiform.com to have a blog.
3. Delfgauw goes on to explain that the developer [software developer of valiform.com] would have written the contents of the blog and that Delfgauw spends a average of “a little bit less” then 30 minutes per work day with the developer.

Exhibit C, Page 25, line 7

Q. Okay. Who wrote -- who would have written the contents of the blog?

A. It probably would have been the developer.

Q. How much time do you spend with the people of that company on the typical day?

A. Again, it could be anywhere from ten minutes to an hour. It could be zero.

Q. So on average per day, would you say 30 minutes per workday?

A. It's probably a little bit less, because the developer has a lot of projects. So when we talk specifically about Validiform, we could go a week without talking about it.

### **The Validiform.com Blog Tells the Story**

If the alleged “opt ins” are not simply made up, and someone/something did “opt in”, the Validiform.com blog<sup>18</sup> tells the story. Emphasis added.

“It’s sad, but there are people out there who are going to try use form spamming to rip you off as an affiliate marketer.

The way they do this is with bots that are programmed to find lead forms on web pages and fill them out. This triggers a “conversion” for them as an affiliate, which technically means you owe them revenue for it.

The issue is the conversion isn’t legitimate, so if you pay out on this conversion, you’re essentially just giving money away to a fraudster that cheated you.

---

<sup>18</sup> Exhibit G archives the varies Validiform.com blog pages. These fit the hearsay exception of Federal Rule of Evidence [801](#)(d)(2).



1 But it can get way worse– and can be much more expensive. See, the form spammers are  
 2 getting more sophisticated, and the bots they’re using are advanced enough to fill in real  
 3 names, real phone numbers, and real email addresses.

4 Since these form fills look legitimate, you’ll likely reach out to these people since (as far  
 5 as you know) they showed interest. The problem is, a bot filled out your form with their  
 6 information, and they have no earthly idea who you are.

7 If you contact them with an offer without their permission, you’re now in violation of  
 8 TCPA regulations and can face up to \$1,500 in fines if the person files a complaint.

9 You need a way to protect your affiliate marketing efforts against form spamming, or it  
 10 could end up costing you a lot of money.”<sup>19</sup>

11 And (emphasis added).

12 “A spambot is a malicious piece of software that is built to crawl your website and find  
 13 specific code, and interact with it, pretending to be human for fraudulent purposes.

14 Spambots can do a number of things, including leaving fake comments, creating fake  
 15 accounts, and executing fake email sign-ups, among many other things.

16 Many Spambots are programmed exclusively to perform fake sign-ups.

17 Since these tasks often only require the user to fill out a few fields, the Spambots are  
 18 programmed to do this automatically. Sometimes these Spambots are coded to invent  
 19 entirely new, fictional user information– but sometimes they’re loaded with real (often  
 20 stolen) information. Some Spambots are so sophisticated that they model human behavior  
 21 before taking action so they’re more difficult to detect.

22 Spambots are never good, but if they’re loaded with stolen, real information to execute  
 23 fake sign-ups it can be especially bad. If you try to send messages to these people, they’ll  
 24 have no idea who you are, and in almost every case, you’ll be breaking the law because  
you don’t have true consent to contact them.”<sup>20</sup>

From the Validiform.com blog: “The baseline method for stopping fake signups is the use  
 of the latest version of a CAPTCHA (or the more advanced ReCAPTCHA). While these  
 tools aren’t perfect, they’re a strong complement to some of the more robust solutions  
 we’ve recommended. A CAPTCHA or ReCAPTCHA forces a website’s user to interact  
with the site with specific clicks that can’t be faked by Spambots easily. This can be

---

<sup>19</sup> Exhibit G, Page 15.

<sup>20</sup> Exhibit G, Page 30

checking a check box, or even selecting a group of similar pictures. **Every site should have a CAPTCHA or ReCAPTCHA as its first line of defense against fake signups.**<sup>21</sup> [emphasis added]

Validiform lists five other ways<sup>22</sup> to block spam bots:

1. Use hidden fields
2. Check for IFrames
3. Use IP Geolocation
4. Use Cookies
5. Filter Proxies/VPNs

**Delfgauw was aware of Spam Bots and did nothing to protect [educationschoolmatching.com](https://www.educationschoolmatching.com) from Spam Bots**

When asked what Defendants did to prevent fraudulent signups on [educationschoolmatching.com](https://www.educationschoolmatching.com), defendants answered:

4	3	<b>INTERROGATORY NO. 14:</b>	For each such "opt-in" that you allege Barton committed
5	4		and for which you suffered injury, please describe every method that was used to prevent the
6	5		signup from being fraudulent.
7	6	<b>ANSWER:</b>	
8	7		Methods to prevent unscrupulous individuals from misusing and profiting from federal
9	8		law have not yet proven to discourage the dishonest, therefore, at this point we trust that
10			those dealing with us are honest and trustworthy.
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			

**AMENDED RESPONSE: A TCPA consent statement is positioned as a gate keeper on the website. Plaintiff had to check the box indicating that he was giving his expressed written consent to receive communication. Without doing so Plaintiff would not have been able to advance to the web from where he provided his phone number and fraudulent contact information.**

<sup>21</sup> Exhibit G, Page 32

<sup>22</sup> Exhibit G, page 16 and page 31

Despite telling others how to prevent most fake sign-ups, defendants answered that they themselves only relied on a TCPA consent statement and a check-box. They did not implement CAPCHA or ReCAPTCHA, use hidden fields, check for IFrames, use IP Geolocation, use cookies, or filter proxies/VPNs that they themselves admit<sup>23</sup> will prevent most fraudulent signups.

Defendants do nothing to prevent fake “opt-ins” on [educationschoolmatching.com](https://educationschoolmatching.com), and once they have the information, they do nothing to check if the phone number entered belongs to the person in possession of the phone<sup>24</sup>:

1	<b>ADMISSION NO. 93:</b>	Admit or deny that if someone “opts in” using
2		<a href="https://educationschoolmatching.com">educationschoolmatching.com</a> , you and the entities under your control simply assume all the
3		information submitted during the “opt in” process is correct.
4	<b>ANSWER:</b>	
5		Admitted. The only way to verify the information would be to contact the consumer and if
6		that consumer is misusing the TCPA to produce a source of income, such contact would
7		be alleged by the person running the scam to be a violation of the TCPA. For the most
		part online marketers trust that those opting in are honest law abiding individuals.

Anyone could have entered *any* phone number on [educationschoolmatching.com](https://educationschoolmatching.com) and the Defendants would have started soliciting it.

Delfgauw could have eliminated all fraudulent “opt ins” by texting the “opted in” phone number with “Thank you for visiting [educationschoolmatching.com](https://educationschoolmatching.com). To receive further messages from us, please respond with “Y”.

This would have eliminated “opt ins” where the person “opting in” wasn’t in possession of the phone.

<sup>23</sup> Exhibit G, Page 31, bottom of the page.

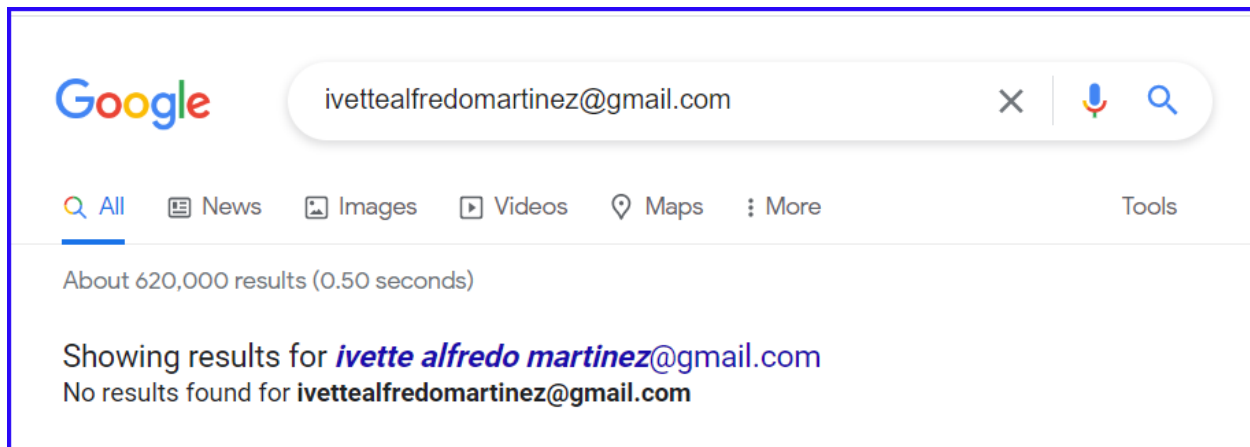
<sup>24</sup> 11.26.2021 CD Delfgauw Admissions 6

# VIII. IVETTEALFREDOMARTINEZ@GMAIL.COM

Table A and B show that the person who “opted in” used email address [ivettealfredomartinez@gmail.com](mailto:ivettealfredomartinez@gmail.com). This is not a random email address. On November 16, 2021, Plaintiff hired George Nobel II (“Nobel”), a licensed Private Investigator working under the business name Paralegal Services of West Michigan to do a “skip trace” on a “Ivette Martinez”.

Paralegal Services of West Michigan returned the “skip trace” shown in Exhibit E<sup>25</sup> the next day. Exhibit E shows that a real person going by Ivette Marquez / Ivette Jimenez / Yvette Jimenez is associated with the phone number at issue (360) 910-1019, and the “opt in” email address [ivettealfredomartinez@gmail.com](mailto:ivettealfredomartinez@gmail.com) (top of Exhibit E, Page 2).

This email address does not appear to be public information. A google search for this email address returns no results.



Plaintiff has testified that prior to the Defendants showing him the email address in discovery, he had never seen it before.

Plaintiff could not “opt in” with an email address he was not aware of.

<sup>25</sup> Plaintiff has redacted the subjects personal information not essential to this motion but will submit the unredacted document to the court if requested.

**Exhibit E shows Ivette Marquez / Ivette Jimenez / Yvette Jiminez is a long time resident of Vancouver Washington.**

**IX. ALL THE PIECES WERE IN PLACE FOR A FRAUDULENT “OPT IN”**

1. Delfgauw testified that he knew bots and people [affiliate marketers] are executing fake sign-ups to get paid.
2. The Validiform.com blog warns that spambots are performing fake sign ups with real information.
3. The Validiform.com blog says at minimum a website should use CAPTCHA / RECAPTCHA to prevent fake sign ups is.
4. Delfgauw admitted [educationschoolmatching.com](https://www.educationschoolmatching.com) didn't use CAPTCHA / RECAPTCHA (or anything else) to prevent spam bots from “opting in”.
5. Delfgauw admits he paid affiliate marketers to deliver “opt ins” to [educationschoolmatching.com](https://www.educationschoolmatching.com).
6. The “opt in” used the first name, last name, email address, and previous phone number of a real Vancouver WA resident to “opt in”.
7. Defendants admit they assume everything submitted in the “opt in” is true.

Plaintiff postulates that if a dishonest affiliate marketer knew Ivette's first name, last name, email address, and previous phone number, that affiliate marketer also knew her Vancouver WA address.

It makes logical sense that if the dishonest affiliate marketer was going to fraudulently “opt in” with Ivette's information to get paid, the dishonest affiliate marketer would use an IP address currently IP geolocated in Ivette's area of residence.

**Defendants' Evidence Points to a Robot “Opt-In”**

Plaintiff draws the Court's attention to a zoomed-in portion of Table A.

ID	Campaign	Day/Time	First	Last	Phone	Email
367588486	12130	2021-04-30 15:50:09	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com
367588483	12130	2021-04-30 15:50:08	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com
362407192	12130	2021-04-13 17:58:07	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com
362407183	12130	2021-04-13 17:58:02	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com
361284364	13690	2021-04-09 18:29:38	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com
358819495	3824	2021-04-01 14:04:11	Ivette	Jimenez	3609101019	ivettealfredomartinez@gmail.com

According to the Defendants, on April 13, 2021, someone “opted in” at 17:58:02 on April 13, 2021, and did it again five second later (blue arrows).

And then, according to the Defendants, on April 30, 2021, someone “opted in” at 15:50:08, and did it again one second later (red arrows).

No reasonable juror could believe Plaintiff (or any other human) is navigating webpages and “opting in” multiple times within one second.

A much more reasonable explanation is that a computer program (spambot) is responsible.

## X. CONCLUSION

The Defendants were careless – they incentivized affiliate marketers to “opt in” phone numbers without checking if the “opt in” was likely from a person or robot. Once they had the information, they simply assumed it was from the person in possession of the phone without doing a single thing to verify it.

Defendants have no admissible evidence. If what they have points to anything, it implicates a spam bot. Even if *Table B* and Exhibit B were admissible, there is less than a scintilla of evidence *Plaintiff* “opted in”. Their entire counterclaim is predicated on a suspicion that Plaintiff “could have opted in” and the hope that a jury might speculate that Plaintiff did. This is insufficient as a matter of law.

1 In the 9<sup>th</sup> circuit, express consent is not an element of a plaintiff's *prima facie* case but is  
 2 an affirmative defense for which the defendant bears the burden of proof. *See In the Matter of*  
 3 *Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991*, 23 F.C.C. Rcd. 559,  
 4 565 (Jan. 4, 2008) (the "2008 Order") ("[W]e conclude that the creditor should be responsible for  
 5 demonstrating that the consumer provided prior express consent.... Should a question arise as to  
 6 whether express consent was provided, the burden will be on the creditor to show it obtained the  
 7 necessary prior express consent."); see also *Grant v. Capital Mgmt. Servs., L.P.*, 449 Fed.Appx.  
 8 598, 600 n.1 (9th Cir. 2011)<sup>26</sup> (" '[E]xpress consent' is not an element of a TCPA plaintiff's  
 9 *prima facie* case, but rather is an affirmative defense for which the defendant bears the burden of  
 10 proof."). See *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, (9th Cir. 2017)<sup>27</sup>.

11 Defendants can't shift their burden of proof by speculating "it's possible" Plaintiff opted  
 12 in. Summary judgement is proper in this case.

13 "[I]n the event the trial court concludes that the scintilla of evidence presented supporting  
 14 a position is insufficient to allow a reasonable juror to conclude that the position more likely than  
 15 not is true, the court remains free to . . . grant summary judgment" *Daubert v. Merrell Dow*  
 16 *Pharmaceuticals, Inc.*<sup>28</sup>, 509 U.S. 579, 596 (1993).

17 "A mere scintilla of evidence will not do, for a jury is permitted to draw only those  
 18 inferences of which the evidence is reasonably susceptible; it may not resort to speculation. See  
 19 *Mutual Fund Investors v. Putnam Management Co.*<sup>29</sup>, 553 F.2d 620, 626 (9th Cir. 1977); *Miller*  
 20

21  
 22 <sup>26</sup> <https://casetext.com/case/grant-v-capital-mgmt-servs-lp>

23 <sup>27</sup> <https://casetext.com/case/van-patten-v-vertical-fitness-grp-llc-3>

24 <sup>28</sup> <https://casetext.com/case/daubert-v-merrell-dow-pharmaceuticals-inc>

<sup>29</sup> <https://casetext.com/case/mutual-fund-investors-v-putnam-management-co>



1 *v. New York Produce Exchange*<sup>30</sup>, 550 F.2d 762, 767 (2 Cir. 1977), cert. denied, 434 U.S. 823,  
 2 98 S.Ct. 68, 54 L.Ed.2d 80 (1977); *Wolf v. Reynolds Electrical Engineering Co.*<sup>31</sup>, 304 F.2d 646,  
 3 649-650 (9 Cir. 1962).” *British Airways Bd. v. Boeing Co.*<sup>32</sup>, 585 F.2d 946, 952 (9th Cir. 1978)

4 Substantial evidence means more than a mere scintilla; it means such relevant evidence  
 5 as a reasonable mind might accept as adequate to support a conclusion. See *Richardson v.*  
 6 *Perales*<sup>33</sup>, 402 U.S. 389, 401 (1971); *Gebhart v. SEC*<sup>34</sup>, 595 F.3d 1034, 1043 (9th Cir. 2010);  
 7 Howard ex rel. Wolff v. Barnhart<sup>35</sup>, 341 F.3d 1006, 1011 (9th Cir. 2003).  
 8

9  
 10  
 11 \_\_\_\_\_  
 s/ Nathen Barton  
 (signed)

\_\_\_\_\_ 6/14/2022  
 (Dated)

12  
 13 Nathen Barton  
 (718) 710 5784  
 14 4618 NW 11<sup>th</sup> Cir  
 Camas WA 98607  
 15

#### 16 CERTIFICATE OF SERVICE

17 I hereby certify that on June 14, 2022, I caused the foregoing document to be  
 18 electronically filed with the Clerk of the Court using the Electronic Filing (CM/ECF) system,  
 19

20 \_\_\_\_\_  
 21 <sup>30</sup> [https://scholar.google.com/scholar\\_case?case=13712592638322142789&hl=en&as\\_sdt=6&as\\_vis=1&oi=scholar](https://scholar.google.com/scholar_case?case=13712592638322142789&hl=en&as_sdt=6&as_vis=1&oi=scholar)

22 <sup>31</sup> <https://casetext.com/case/wolf-v-reynolds-electrical-engineering-co>

23 <sup>32</sup> <https://casetext.com/case/british-airways-bd-v-boeing-co>

24 <sup>33</sup> <https://casetext.com/case/richardson-v-perales>

<sup>34</sup> <https://casetext.com/case/gebhart-v-sec-2>

<sup>35</sup> <https://casetext.com/case/howard-ex-rel-wolff-v-barnhart>

1 which will send notification of such filing to all counsel of record and all pro se parties registered  
2 to use the CM/ECF system.

3  
4 s/ Nathen Barton

Nathen Barton

6/14/2022

(Dated)